

AUSAs: Kevin Mead and Micah Fergenson

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

NATHAN AUSTAD,
a/k/a "Snoopy," and
KAMERIN STOKES,
a/k/a "TheMFNPlug,"

Defendants.

24 MAG 155**SEALED COMPLAINT**Violations of 18 U.S.C. §§ 371, 1030,
1349, 1343, 1028A, and 2COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

MICHAEL GASSERT, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

1. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a "Snoopy," and KAMERIN STOKES, a/k/a "TheMFNPlug," the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, a violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(a)(4).

2. It was a part and an object of the conspiracy that NATHAN AUSTAD, a/k/a "Snoopy," and KAMERIN STOKES, a/k/a "TheMFNPlug," the defendants, and others known and unknown, would and did intentionally access a computer without authorization, and exceed authorized access, and thereby would and did obtain information from a protected computer, which was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i) & (iii).

3. It was further a part and an object of the conspiracy that NATHAN AUSTAD, a/k/a "Snoopy," and KAMERIN STOKES, a/k/a "TheMFNPlug," the defendants, and others known and unknown, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value totaling more than \$5,000 during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

Overt Act

4. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere:

a. In or about November 2022, NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, used leaked credentials to access victims’ electronic betting accounts on a fantasy sports and sports betting website (the “Betting Website”).

b. In or about November 2022, KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendant, sold access to stolen credentials to access victims’ electronic betting accounts on the Betting Website.

(Title 18, United States Code, Section 371.)

COUNT TWO

(Computer Fraud - Unauthorized Access to a Protected Computer to Further Intended Fraud)

5. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendants, knowingly and with the intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value totaling more than \$5,000 during a one-year period, to wit, AUSTAD and STOKES obtained unauthorized access to victims’ electronic betting accounts on the Betting Website and sold the means of unauthorized access to those accounts—namely, account login information, along with instructions for how to drain funds from the compromised accounts—to others who used that information to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), and 2.)

COUNT THREE

(Computer Fraud - Unauthorized Access to a Protected Computer)

6. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendants, intentionally accessed a computer without authorization, and exceeded authorized access, and thereby obtained information from a protected computer, which was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded \$5,000, to wit, AUSTAD and STOKES obtained unauthorized access to victims’ electronic betting accounts on the Betting Website and obtained information from those accounts, namely account login information, which he sold to others who used that

information to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1030(a)(2)(c), 1030(c)(2)(B)(i), and 2.)

COUNT FOUR
(Wire Fraud Conspiracy)

7. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

8. It was a part and an object of the conspiracy that NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendants, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, AUSTAD and STOKES agreed with others to engage in a scheme to obtain unauthorized access to victims’ electronic betting accounts on the Betting Website under false pretenses in order to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Section 1349.)

COUNT FIVE
(Wire Fraud)

9. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendants, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, AUSTAD and STOKES engaged in a scheme to obtain unauthorized access to victims’ electronic betting accounts on the Betting Website under false pretenses in order to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT SIX
(Aggravated Identity Theft)

10. In or about November 2022, in the Southern District of New York and elsewhere, NATHAN AUSTAD, a/k/a “Snoopy,” and KAMERIN STOKES, a/k/a

“TheMFNPlug,” the defendants, knowingly transferred, possessed, and used, without lawful authority, means of identification of another person, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, AUSTAD and STOKES transferred and used, and aided and abetted the use of, the identifying information of other people during and in relation to the computer intrusion and wire fraud offenses charged in Counts One through Five of this Complaint.

(Title 18, United States Code, Sections 1028A(a)(1) and (b), and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

11. I am a Special Agent with the FBI. This affidavit is based on my personal participation in the investigation of this matter, my conversations with other law enforcement agents, witnesses and others, as well as my examination of reports and records. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview

12. In November 2022, hackers launched a credential stuffing attack on the Betting Website (the “Betting Website Attack”) and thereby obtained access to tens of thousands of Betting Website user accounts (the “Victim Accounts”).

13. During a credential stuffing attack, a cyber threat actor collects stolen credentials, or username and password pairs, obtained from other large-scale data breaches of other companies, which can be purchased on the darkweb.¹ The threat actor then systematically attempts to use those stolen credentials to obtain unauthorized access to accounts held by the same user with other companies and providers, in order to compromise accounts where the user has maintained the same password.²

14. The hackers then sold access to the Victim Accounts through various websites that market and sell illegal account credentials. The buyers of those credentials accessed the Victim Accounts and withdrew approximately \$635,000 in total from the Victim Accounts.

15. Law enforcement identified NATHAN AUSTAD, a/k/a “Snoopy,” the

¹ Darkweb marketplaces are underground e-commerce websites that offer contraband over the Internet. These marketplaces use technology, including The Onion Router or “Tor” network, and cryptocurrency, to protect the anonymity of the individuals that operate the marketplace, as well as the vendors and customers who use the marketplace.

² To give an example of how a credential stuffing attack might work, an individual might purchase a list of 100,000 usernames and passwords obtained from a hack or data breach of an email service provider, and then use a computer program to rapidly attempt to log into financial accounts using each of those 100,000 linked usernames and passwords.

defendant, as one of the individuals who initially hacked the Betting Website and sold access to the Victim Accounts based on the following, in substance and in part:

a. Law enforcement reviewed electronic devices belonging to Joseph Garrison, one of the individuals who committed the Betting Website Attack.³ Those devices contain chats stating that an individual named “Snoopy” initially committed the Betting Website Attack, and metadata on one of the files used to commit the attack shows that the file was created by “Snoopy.”

b. Law enforcement also located a website controlled by “Snoopy” that sold access to stolen accounts, and chats found on Garrison’s devices establish that “Snoopy” was selling Victim Accounts on that website.

c. Subpoena return evidence from Apple, Cloudflare, and Discord establishes that AUSTAD is “Snoopy.”

d. Law enforcement searched AUSTAD’s home and recovered extensive evidence, set forth in further detail below, that he was “Snoopy” and that he committed the Betting Website Attack.

16. Law enforcement identified KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendant, as one of the individuals who bought and resold access to the Victim Accounts based on the following, in substance and in part:

a. Website, Instagram, and Telegram records establish that an individual who uses the alias “TheMFNPlug” operated a website on which he sold access to the Victim Accounts.

b. Garrison’s devices contain messages between Garrison and “TheMFNPlug,” establishing that Garrison sold stolen accounts to “TheMFNPlug” so that “TheMFNPlug” could resell those accounts on his website.

c. Law enforcement identified STOKES as “TheMFNPlug” based on subpoena returns and Instagram posts, as detailed below.

The Credential Stuffing Attack on the Betting Website

17. Based on law enforcement communications with employees of the Betting Website and my review of records provided by the Betting Website, I have learned the following, in substance and in part:

a. The Betting Website is a fantasy sports and sports betting company.

³ Garrison has pleaded guilty in this district to one count of conspiracy to commit computer intrusions in connection with the Betting Website Attack. *United States v. Garrison*, 23 Cr. 597 (LAK).

b. On or about November 18, 2022, the Betting Website was subjected to a credential stuffing attack (*i.e.*, the Betting Website Attack). In connection with the Betting Website Attack, there were a series of attempts to log into the Betting Website accounts using a large list of credentials.

c. I further know from my training and experience that when individuals successfully execute a credential stuffing attack, they will frequently sell access to many of the accounts they have illegally accessed on various websites that deal in hacked accounts.

d. In connection with the Betting Website Attack, approximately 60,000 Victim Accounts at the Betting Website were successfully compromised.

e. In some instances, the individuals who unlawfully accessed the Victim Accounts were able to add a new payment method on the account, deposit \$5 into that account through the new payment method to verify that method, and then withdraw all the existing funds in the Victim Account through the new payment method (*i.e.*, to a newly added financial account belonging to the hacker), thus stealing the funds in the Victim Account. Using this method, the hackers stole approximately \$635,000 from approximately 1,600 Victim Accounts.

18. Based on my review of records provided by the Betting Website, I have learned, in substance and in part, that at least 30 of the 60,000 Victim Accounts accessed via the Betting Website Attack have listed addresses in the Southern District of New York. I have additionally interviewed approximately four individuals who confirmed that they were victims of the Betting Website Attack and that they reside in the Southern District of New York.

Undercover Purchases of Betting Website Credentials

19. I know from my training and experience that when a large number of accounts are hacked, as in the Betting Website Attack, the attackers frequently sell access to those accounts to websites that traffic in stolen accounts, which are frequently referred to as “shops” (the “Shop Websites”). The Shop Websites then in turn resell access to stolen accounts to individual purchasers.

20. Based on discussions with employees of the Betting Website and an undercover law enforcement officer (the “UC”), as well as my review of records relating to an undercover operation, I have learned the following, in substance and in part:

a. On or about January 9, 2023, the UC observed Betting Website credentials for sale on a website (“Website-1”). The UC purchased two sets of those credentials—meaning usernames and passwords for two Victim Accounts—for approximately \$11 (the “Website-1 Credentials”). The UC made the purchase of credentials from an office located in the Southern District of New York and the credentials were transmitted to the UC and downloaded by the UC from the office located in the Southern District of New York. Law enforcement confirmed with the Betting Website that the email addresses in the Website-1 Credentials belonged to active Betting Website accounts.

b. Law enforcement observed that stolen Betting Website credentials were also available for purchase on another website (“Website-2”).

The Garrison Search and Evidence that Garrison was a Member of the Conspiracy to Hack the Betting Website

21. I know from my involvement in the investigation that on or about February 23, 2023, law enforcement executed a search pursuant to a judicially authorized search warrant at an address in Wisconsin where Joseph Garrison resides (the “Garrison Search”). In that search, law enforcement recovered and searched several devices belonging to Garrison, including his computer (the “Garrison Computer”) and cellphone (the “Garrison Phone”).

22. The following evidence from the Garrison Search establishes that Garrison participated in the Betting Website Attack:

a. Law enforcement located the programs OpenBullet and SilverBullet on the Garrison Computer. I know from my training and experience that OpenBullet and SilverBullet are programs frequently used to execute credential stuffing attacks.

b. I further know from my training and experience that to launch a credential stuffing attack using OpenBullet or SilverBullet, an individual needs both a “wordlist” and a “config.” A “wordlist” contains a series of username and password combinations, while a “config” is a script that will run the wordlist through the log-in page of a particular website.

c. On the Garrison Computer, law enforcement located 11 separate configs for the Betting Website. Metadata shows that the earliest creation date for one of those configs was November 17, 2022, approximately one day before the Betting Website Attack.

d. On the Garrison Computer, law enforcement also located approximately 700 separate configs designed for credential stuffing attacks against dozens of other company websites.

e. On the Garrison Computer, law enforcement located at least 69 wordlists which contained at least 38,484,088 individual username and password combinations.⁴

f. On the Garrison Computer, law enforcement located a number of photos that provided instructions as to how to extract money from stolen Betting Website accounts. Law enforcement observed those same photos on Shop Websites that sold stolen Betting Website accounts. Those photos were created using a particular program that: (a) indicated that Garrison had created the photos; and (b) indicated that the photos had been created on or about November 18, 2022, the date of the Betting Website Attack.

g. On the Garrison Phone, law enforcement also located a number of

⁴ Some of these combinations are likely duplicates.

chats with co-conspirators about how to execute the Betting Website Attack, how to profit from the Betting Website Attack by extracting funds from the Victim Accounts directly or by selling access to the Victim Accounts, how Garrison would provide access to stolen accounts to co-conspirators that they could then resell on Shop Websites, how Garrison enjoyed executing credential stuffing attacks, and Garrison's belief that law enforcement would not catch or prosecute him for his credential stuffing attacks.

**Evidence that "Snoopy" Hacked the Betting Website
and that "Snoopy" is NATHAN AUSTAD**

I. Evidence from the Garrison Search and the Snoopy Shop Website that "Snoopy" Hacked the Betting Website

23. As explained above, I know from my training and experience that a "config" file is a script used to launch a credential stuffing attack on a website. As described above, law enforcement recovered multiple config files for the Betting Website on the Garrison Computer. Metadata shows that the earliest creation date for one of those config files was November 17, 2022, approximately one day before the Betting Website Attack. Further, metadata shows that the author of the Betting Website config file was listed as "snoopy#0420."

24. On the Garrison Phone, law enforcement recovered Telegram⁵ chats between Garrison and a coconspirator ("CC-1"):

Date	Sender	Message
11/17/2022	Garrison	do u have captcha ⁶
11/17/2022	CC-1	Uh
11/17/2022	CC-1	not rly
11/17/2022	CC-1	for what site u need
11/17/2022	Garrison	[the Betting Website]
11/17/2022	CC-1	Eh
11/17/2022	CC-1	its shit
11/17/2022	CC-1	don't bother
11/17/2022	Garrison	i have bypass ⁷
11/17/2022	CC-1	2fa? ⁸

⁵ Telegram is an encrypted messaging platform.

⁶ Based on my training and experience and involvement in the investigation, I understand "captcha" to be an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart," a verification tool at the log-in stage in which a human must correctly identify, for example, altered text in a picture, to ensure that a bot is not attempting to log in. Successful credential stuffing attacks frequently rely on overcoming CAPTCHA protections.

⁷ Based on my training and experience and involvement in the investigation, I understand "bypass" to refer to a method to avoid anti-hacking protocols by websites, such as two-factor authentication and CAPTCHAs.

⁸ Based on my training and experience and involvement in the investigation, I understand "2fa" to refer to "two-factor authentication," a protocol to make hacking accounts more difficult.

11/17/2022	CC-1	<i>snoopy</i>
11/17/2022	CC-1	Bypass
11/17/2022	CC-1	Jeez
11/17/2022	CC-1	u rich
[]		
11/18/2022	Garrison	if u get captcha
11/18/2022	Garrison	we can do
11/18/2022	Garrison	[the Betting Website]
11/18/2022	Garrison	Too
11/18/2022	CC-1	i have solver
11/18/2022	CC-1	it's just
11/18/2022	CC-1	[the Betting Website]
11/18/2022	CC-1	doesn't hit
11/18/2022	CC-1	for me
11/18/2022	Garrison	u need bypass
11/18/2022	Garrison	i have it
[]		
11/18/2022	Garrison	[Messaged lines of code that I understand, from my training and experience and involvement in the investigation, are designed to be used against the Betting Website]
[]		
11/18/2022	Garrison	<i>snoopy got like</i>
11/18/2022	Garrison	<i>20k worth of accs</i> ⁹
11/18/2022	Garrison	in like 3hrs checking
11/18/2022	CC-1	imma get more
11/18/2022	Garrison	give me bulk ill sell on other shops ¹⁰
11/18/2022	Garrison	i have a bunch lined up
11/18/2022	Garrison	ill give u profit
[]		
11/18/2022	CC-1	[Messages a photo of SilverBullet running against the Betting Website]

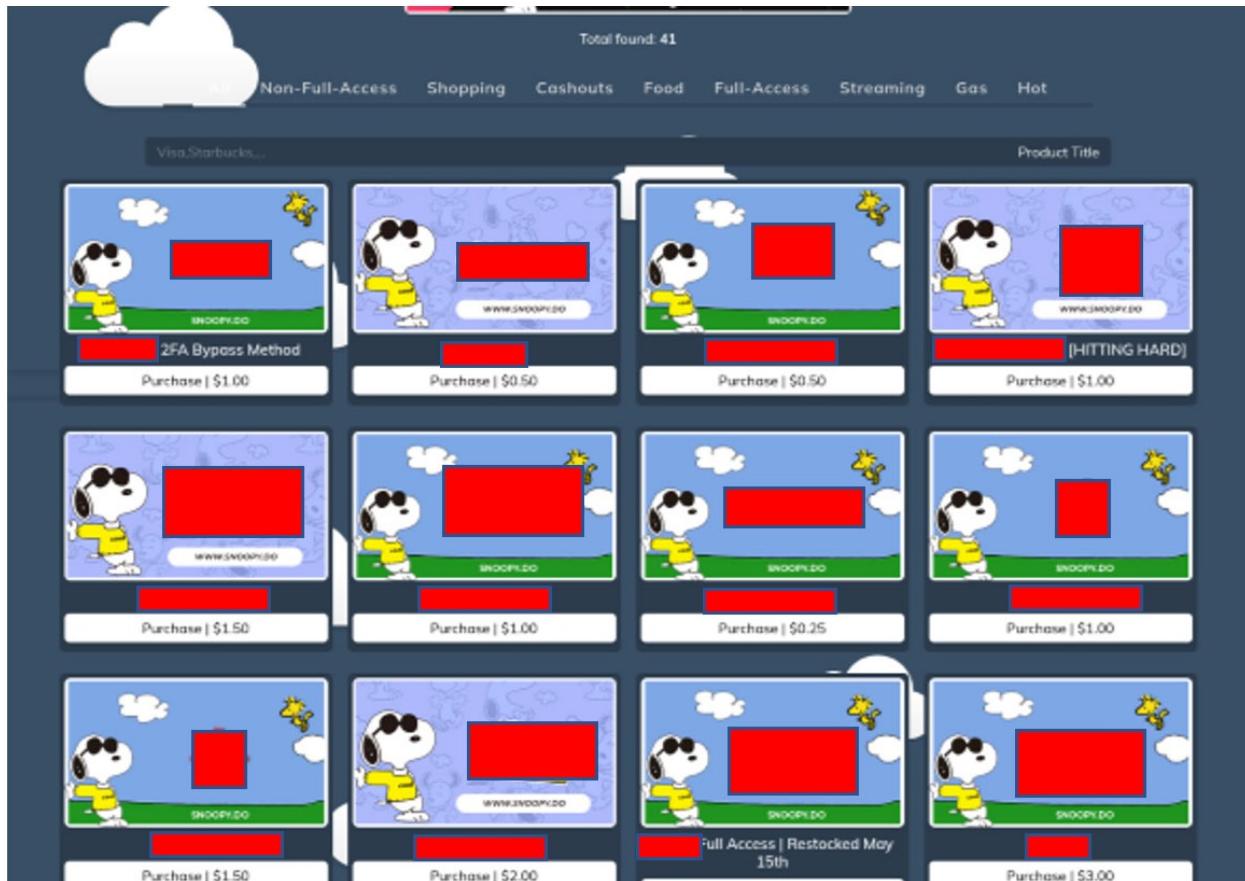
(Emphasis added.)

25. As described above, stolen accounts are frequently sold on websites that traffic in such accounts, i.e., the Shop Websites. Law enforcement has located a website at the address snoop.fo that sells access to such stolen accounts and uses branding related to the Peanuts

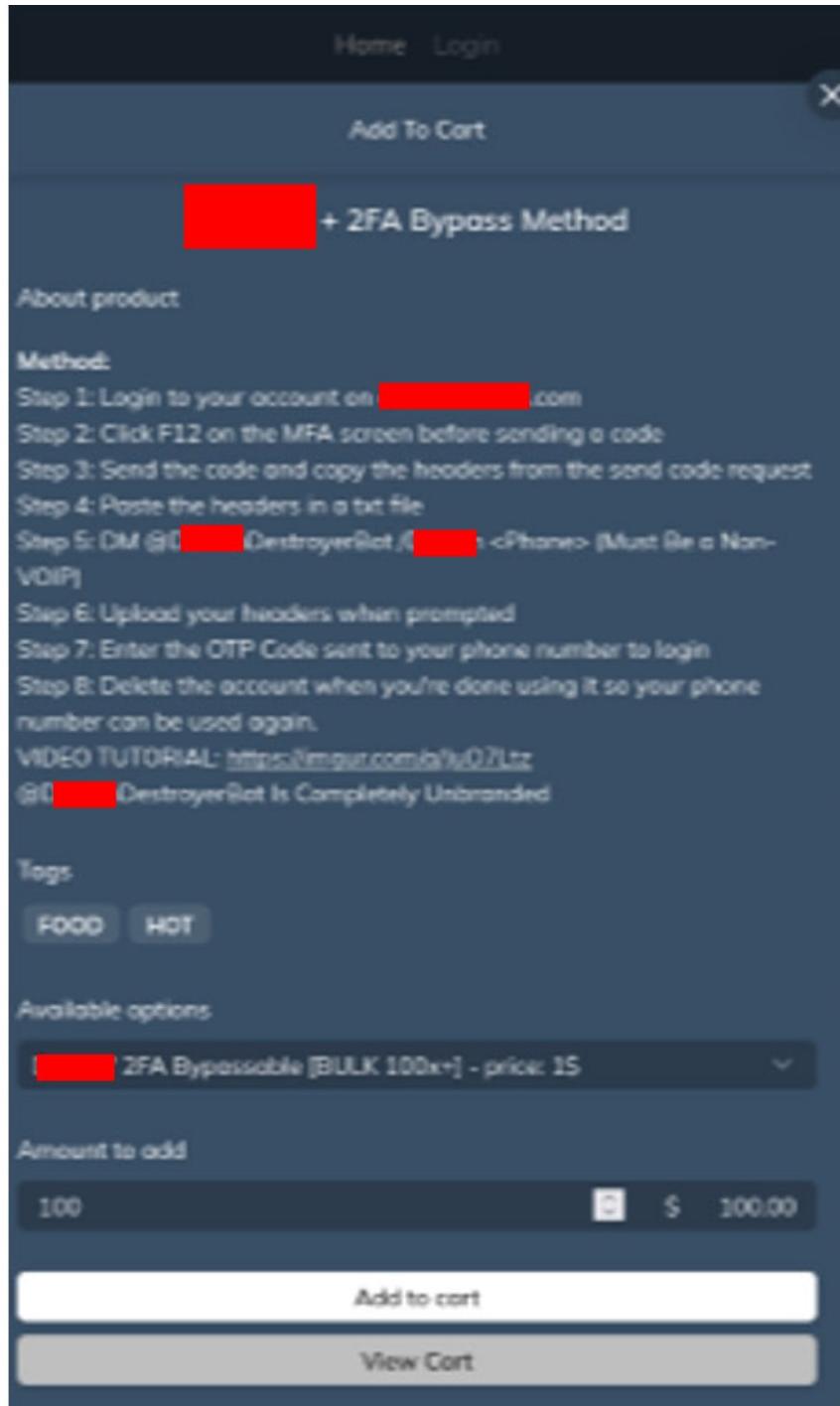
⁹ Based on my training and experience and involvement in the investigation, I understand “accs” to be short for “accounts,” and to refer to individual user accounts that have been successfully illegally accessed.

¹⁰ Based on my training and experience and involvement in the investigation, I understand terms like “shop” and “acc shop” to refer in this context to websites that sell stolen log-in credentials, such as the “Snoopy Shop Website” discussed below.

comic strip character Snoopy (the “Snoopy Shop Website”). Below are photos of the Snoopy Shop Website that show various categories of stolen accounts for sale, as well as instructions for how to access, for example, stolen accounts at a fast-food restaurant after they have been purchased.¹¹



¹¹ As to each company for which stolen accounts are available for purchase, the name and logo of the companies have been redacted. The photos do not show the ability to purchase stolen Betting Website accounts.



26. On the Garrison Phone, law enforcement also recovered a Telegram chat thread for users of the Snoopy Shop Website on Telegram, (the “Snoopy Shop Telegram Thread”). In the Snoopy Shop Telegram Thread, the owner of the Snoopy Shop Website messaged on November 17, 2022—the day before the Betting Website Attack—“[Betting Website] withdrawal 2fa bypass just found! Selling to 1 customer only \$5k.” Based on my training and experience and involvement in the investigation, I understand this message thread to mean that “Snoopy” has found a method to access Betting Website accounts and to withdraw funds that bypassed two-

factor authentication, and that he is willing to sell that method for \$5,000.

II. Subpoena Return Evidence that “Snoopy” is NATHAN AUSTAD

27. I have reviewed a subpoena return from the web security service Cloudflare for the Snoopy Shop Website. The subpoena return shows the Cloudflare account associated with the Snoopy Shop Website registered using a particular Internet Protocol (“IP”) address 72.106.207.192 (the “192 IP Address”) and listing a particular physical address (the “Minnesota Address”).

28. I have reviewed a subpoena return from Apple for an account in the name of “Nathan Austad,” which shows that the Apple account used the 192 IP Address—the same one used for the Cloudflare account on the Snoopy Shop Website—on or about February 11, 2023.

29. On the Snoopy Shop Telegram Thread, I have reviewed a message from the owner of the Snoopy Shop Website from on or about October 24, 2022, that says, “!Snoopy#0420 is my new discord ‘snoopy#0420’ was banned and I have no alts.” As described above, metadata shows that the author of the Betting Website config file used in the hack was also identified as “snoopy#0420.” I know from my training and experience that Discord is a messaging service. I have reviewed a subpoena return for Discord for the username !Snoopy#0420 that shows that the user registered the username with the Minnesota Address.

III. Evidence from the Austad Search

30. I know from my involvement in the investigation that on or about November 7, 2023, law enforcement executed a search pursuant to a judicially authorized search warrant at an address in Minnesota where NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, resides (the “Austad Search”). In that search, law enforcement recovered and searched several electronic devices belonging to Austad (the “Austad Devices”)

31. NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, told law enforcement, in substance and in part, that he used to use “Snoopy” as an online alias. Law enforcement further observed multiple items referring to the Peanuts character Snoopy in AUSTAD’s bedroom.

32. On the Austad Devices, law enforcement located evidence that NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, was logged into and controlled a Telegram account that used the username “Snoopy.” Law enforcement also located evidence that AUSTAD was logged into and controlled a CashApp account with the username “\$SnoopyDotDo” and a Discord account with the username “snoppyfo #0.”

33. On the Austad Devices, law enforcement recovered the following Telegram chats between NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, and another coconspirator (“CC-2”) from one day after the Betting Website Attack:

Date	Sender	Message
------	--------	---------

11/19/2022	CC-2	Let me buy some [Betting Website] bulk? ¹²
11/19/2022	AUSTAD / "Snoopy"	Yeah I can \$5 a log for over 100
11/19/2022	AUSTAD / "Snoopy"	Snoopy.gg for anything under 50 logs

I understand these messages to be a request by CC-2 to buy access to Victim Accounts. I understand AUSTAD's response to mean that he will sell access to large number of accounts (more than 100 at a time) directly, or CC-2 can purchase smaller numbers of accounts from AUSTAD's website, Snoopy.gg, which I understand to refer to the Snoopy Shop Website.¹³

34. On the Austad Devices, law enforcement recovered the following Telegram chats between NATHAN AUSTAD, a/k/a "Snoopy," the defendant, and another coconspirator ("CC-3") from three days after the Betting Website Attack:

Date	Sender	Message
11/21/2022	CC-3	U have [Betting Website] and [name of another betting website]? Or any other cashouts?
11/21/2022	AUSTAD / "Snoopy"	nah just sold all
11/21/2022	CC-3	Configs i mean
11/21/2022	AUSTAD / "Snoopy"	Oh yeah
11/21/2022	AUSTAD / "Snoopy"	[Betting Website]

I understand these messages to be a request by CC-3 to purchase Victim Accounts for the Betting Website, or to purchase a config file for the Betting Website so that CC-3 can conduct his own credential stuffing attack. I understand AUSTAD to respond that he has sold all the Victim Accounts he has access to, but has the config file for the Betting Website available.

35. On the Austad Devices, law enforcement recovered a message NATHAN AUSTAD, a/k/a "Snoopy," the defendant, sent on or about December 2, 2022, in which AUSTAD posted a link to an ESPN article with the headline, "Source: FBI investigating cyberattack of online sportsbooks," which referred to an FBI investigation into the Betting Website Hack. AUSTAD and a coconspirator ("CC-4") then exchanged the following messages:

¹² CC-1 uses only part of the name of the Betting Website in the redacted text, but I understand from the timing of the messages and the context that CC-1 referred to the Betting Website

¹³ A top level domain refers to the ending of a website address, such as .com, .org, .biz, or .edu. I understand from my training and experience and involvement in the investigation that top level domain of the Snoopy Shop Website changed over time, likely because hosting services shut down the website when they became aware of its fraudulent nature, and AUSTAD was therefore forced to migrate it to another hosting service with a different top level domain. This Complaint refers to the Snoopy Shop Website as a single website, even though the Snoopy Shop Website used multiple top level domains over time.

Date	Sender	Message
12/2/2022	AUSTAD / "Snoopy"	everyone shouldve been prepared for this before cashing out lol
12/3/2022	CC-4	lol fbi can't do shit

36. On the Austad Devices, law enforcement recovered the following Telegram chats between NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, and another coconspirator (“CC-5”) from several months after the Betting Website Attack:

Date	Sender	Message
5/19/2023	AUSTAD / "Snoopy"	they all just shaking in their boots
5/19/2023	CC-5	XD
5/19/2023	AUSTAD / "Snoopy"	like we didnt know the risk when we started lol
5/19/2023	AUSTAD / "Snoopy"	everyone knows their committing fraud
[]		
5/19/2023	AUSTAD / "Snoopy"	The new incident was yesterday
5/19/2023	AUSTAD / "Snoopy"	We talked to joey 3 days ago in VC

I understand the references to a “new incident” regarding “joey” to refer to the arrest of Joseph Garrison on or about May 18, 2023, in connection with the Betting Website Attack.

37. On the Austad Devices, law enforcement recovered a message thread between NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, and several coconspirators in which they discuss a new credential stuffing attack several months after the Betting Website Attack. On or about September 13, 2023, AUSTAD messaged, “That’s what we did for [Betting Website],” which I understand to mean that AUSTAD used the same type of hacking method in the Betting Website Attack.

38. On the Austad Devices, law enforcement located approximately 3,777,641 combinations of usernames and passwords. On the Austad Devices, law enforcement further located approximately 116 “config” files. As described above, “config” is a script that will run the wordlist through the log-in page of a particular website. While none of the configs were for the Betting Website, they were for the websites of a number of other corporations, which indicates that NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, committed or was planning to commit multiple other credential stuffing attacks.

39. I know the following from my review of the browser history on the Austad Devices:

- a. On or about September 6, 2023, NATHAN AUSTAD, a/k/a

“Snoopy,” the defendant, visited the “admin dashboard” of the Snoopy Shop Website, which I know from my training and experience indicates that he controlled the Snoopy Shop Website.

b. On or about September 9, 2023, AUSTAD searched, “statute of limitations on fraud.”

c. In or about October and November 2023, AUSTAD used online artificial intelligence image generation tools to generate images using the following prompts, which I understand that AUSTAD used to brag about the success and profitability of his criminal activity:

i. “8k¹⁴ hyper-realistic digital art snoopy hacking into 8k hyper-realistic computer with hacker stuff on the screen”

ii. “8k hyper realistic snoopy designed jet but instead of smoke trails it has money trails”

iii. “100 bill hyper realistic but instead of the president its snoopy”

40. During the search of the address where NATHAN AUSTAD, a/k/a “Snoopy,” the defendant, resided, law enforcement also located several physical items with an image of the Peanuts comic strip character Snoopy, further confirming AUSTAD’s use of that alias. Photos of certain of those items are below:



41. On the Austad Devices, law enforcement located cryptocurrency wallets that had received cryptocurrency worth approximately \$465,000 between January 1, 2021, and

¹⁴ Based on my training and resolution, I understand that “8k” refers to how high the resolution of the requested image will be.

December 9, 2022. While a substantial portion of those funds were received before the Betting Website Attack, in light of the substantial evidence of additional credential stuffing attacks described herein, I understand that all or most of the funds were the proceeds of similar credential stuffing attacks and/or the sale of stolen accounts as a result of such attacks.

Evidence that “TheMFNPlug” Sold Access to Victim Accounts from the Betting Website and that “TheMFNPlug” is KAMERIN STOKES

I. Evidence from the Garrison Search that “TheMFNPlug” Sold Access to Victim Accounts

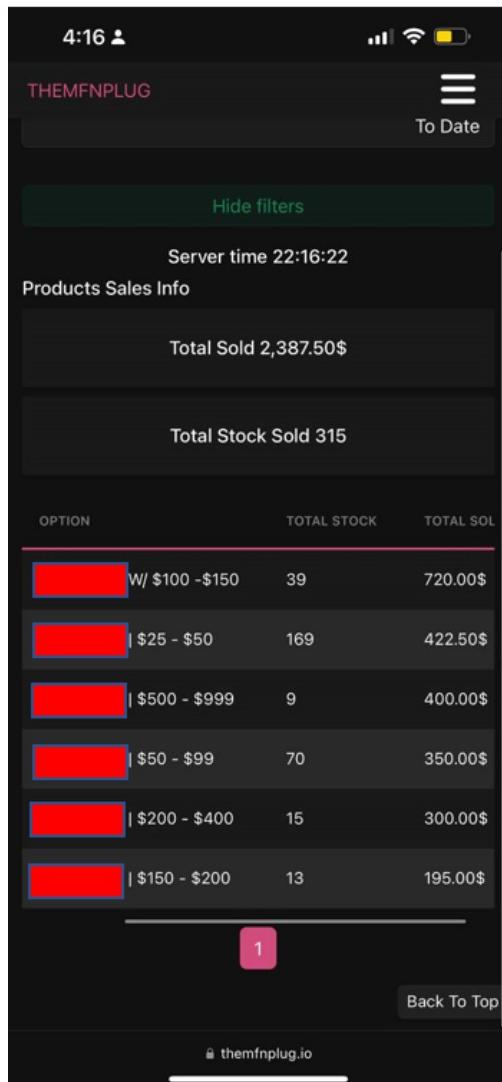
42. On the Garrison Phone, law enforcement recovered Telegram chats between Garrison and a user with the name “themfnplug”:

Date	Sender	Message
11/18/2022	Garrison	Hi
11/18/2022	Garrison	I got
11/18/2022	Garrison	[the Betting Website]
11/18/2022	themfnplug	No captcha ?
11/18/2022	Garrison	I have captchaless vm
11/18/2022	Garrison	I can stock if u want
11/18/2022	themfnplug	Yesss pls
11/18/2022	themfnplug	I have method
11/18/2022	themfnplug	And all
11/18/2022	Garrison	I made the method
11/18/2022	Garrison	[the Betting Website] Method Step 1; Go to account settings and enable 2fa through the phone number Put your own phone number, this is how you bypass 2fa to cashout the account. https://i.imgur.com/K9ehpjV.png Step 2; Add your own payment method and add \$5 to account balance (similar to fanduel) Step 3; Withdraw the balance of the account to any payment method https://i.imgur.com/rsR8ZM5.png Step 4; Send code to SMS instead of email https://i.imgur.com/Pq8IEeN.png Step 5; Enjoy your money! https://i.imgur.com/CzUcDqS.png
11/18/2022	Garrison	Ima take my dog out then ill stock u
11/18/2022	Garrison	I got a fuck ton of stock
11/18/2022	themfnplug	Okay bet
11/18/2022	themfnplug	And I can show full stats of what's sold cuz of my custom site
11/18/2022	themfnplug	#stats op

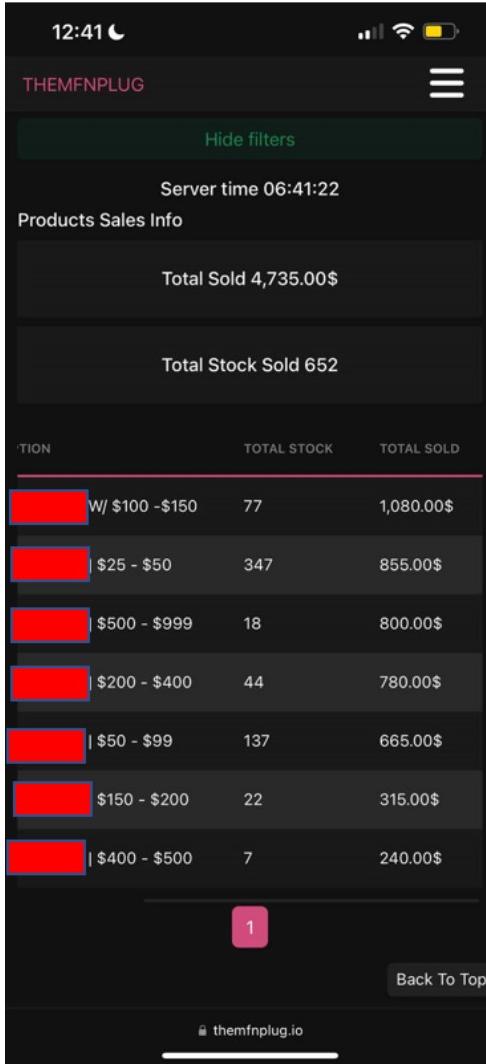
11/18/2022	Garrison	Lmao
11/18/2022	Garrison	Lemme sort this shit
11/18/2022	themfnplug	Damn I jus realized this the same method I did wit FanDuel
11/18/2022	Garrison	Nah u need to add
11/18/2022	Garrison	Phone 2fa
11/18/2022	Garrison	On this one
11/18/2022	themfnplug	okok
11/18/2022	Garrison	[email and password omitted] Balance = \$476.30 [email and password omitted] Balance = \$439.15 [email and password omitted] Balance = \$421.10
11/18/2022	Garrison	Use these for drop
11/18/2022	Garrison	Or something
11/18/2022	Garrison	How u wanna price
11/18/2022	Garrison	Over 1k ones
11/18/2022	themfnplug	People saying Ssn but I assume they clipping or it's web I'll probably do 25-35%
11/18/2022	Garrison	ssn is on like not even 1% of accs and only on app
11/18/2022	Garrison	Yea thought so
11/18/2022	Garrison	Web way easier to hit than app
11/18/2022	Garrison	[messages photo showing: 25-50 x 175.txt 50-99 x 67.txt 100-150 x 45.txt 150-200 x 18.txt 200-400 x 18.txt 500-999 x 10.txt 1k+ x 8.txt]
11/18/2022	Garrison	Ill ad up total value
11/18/2022	Garrison	Okok
11/18/2022	Garrison	[Messages file titled 1k+ x 8.txt containing a list of 8 account names and passwords, with each account having at least \$1,000] ¹⁵
11/18/2022	Garrison	[Messages file titled 25-50 x 175.txt containing a list of 175 account names and passwords, with each account having between \$25-\$50]
11/18/2022	Garrison	[Messages file titled 50-99 x 67.txt containing a list of 67 account names and passwords, with each account having between \$50-\$99]
11/18/2022	Garrison	[Messages file titled 100-150 x 45.txt containing a list of 45 account names and passwords, with each account having between \$100-\$150]

¹⁵ This file contained an account name and password for a victim (“Victim-1”) who resides in the Southern District of New York.

11/18/2022	Garrison	[Messages file titled 150-200 x 18.txt containing a list of 18 account names and passwords, with each account having between \$150-\$200]
11/18/2022	Garrison	[Messages file titled 200-400 x 18.txt containing a list of 18 account names and passwords, with each account having between \$200-\$400]
11/18/2022	Garrison	[Messages file titled 500-999 x 10.txt containing a list of 10 account names and passwords, with each account having between \$500-\$999]
11/18/2022	themfnplug	What you recommend pricing like
11/18/2022	Garrison	25% is fine
11/18/2022	themfnplug	Okok
11/18/2022	Garrison	O this is smaller than I thought
11/18/2022	Garrison	31k
11/18/2022	Garrison	Of acs
11/18/2022	themfnplug	kk
[]		
11/20/2022	Garrison	Do u need more
11/20/2022	Garrison	stock
11/20/2022		YEA
11/20/2022	Garrison	[Messages file titled 500-999 x 9.txt containing a list of 9 account names and passwords, with each account having between \$500-\$999]
11/20/2022	Garrison	[Messages file titled 25-50 x 182.txt containing a list of 182 account names and passwords, with each account having between \$25-\$50]
11/20/2022	Garrison	[Messages file titled 50-99 x 72.txt containing a list of 72 account names and passwords, with each account having between \$50-\$99]
11/20/2022	Garrison	[Messages file titled 100-150 x 41.txt containing a list of 41 account names and passwords, with each account having between \$100-\$150]
11/20/2022	Garrison	[Messages file titled 150-200 x 11.txt containing a list of 11 account names and passwords, with each account having between \$150-\$200]
11/20/2022	Garrison	[Messages file titled 200-400 x 30.txt containing a list of 30 account names and passwords, with each account having between \$200-\$400]
11/20/2022	Garrison	[Messages file titled 400-500 x 7.txt containing a list of 7 account names and passwords, with each account having between \$400-\$500]
11/20/2022	Garrison	How were ur sales on it
11/20/2022	themfnplug	Sending now
11/20/2022	themfnplug	[messages the below image file]



11/20/2022	Garrison	What cut can u toss me
11/20/2022	Garrison	500?
11/20/2022	themfnplug	Whatever you want
11/20/2022	Garrison	Im chill with 500
11/20/2022	Garrison	Im only selling bulk to pay for captcha
11/20/2022	Garrison	All my profit gonna come from cashing
<hr/>		
11/21/2022	themfnplug	Send yo btc addy
11/21/2022	themfnplug	[messages the below image file]



On or about November 21, 2022, Garrison sent “TheMFNPlug” a third set of text files containing usernames, passwords, and account balances for Betting Website accounts. In total, the text files Garrison sent “TheMFNPlug” had a total listed account value of approximately \$125,965.53.

II. Evidence from Websites, Instagram, and Telegram that “TheMFNPlug” Sold Stolen Betting Website Accounts

43. As described in additional detail below, an individual who uses the alias “TheMFNPlug” operated a Shop Website (the “MFNPlug Shop”) and sold access to stolen Betting Website accounts for sale on that site.

44. Below are photographs taken from TheMFNPlug Shop, with the URL themfnplug.io. The photos depict various stolen accounts for sale on the MFNPlug Shop, although these photos do not depict Betting Website accounts for sale:

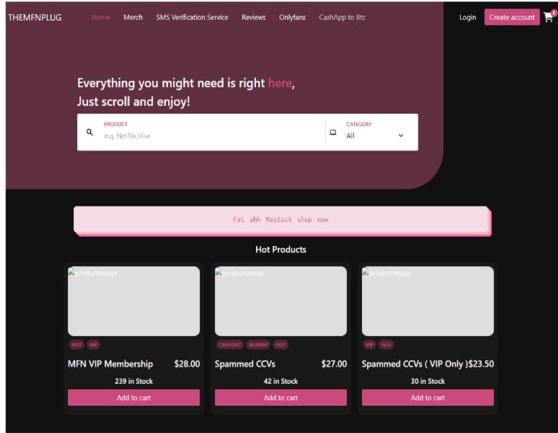


Photo-1

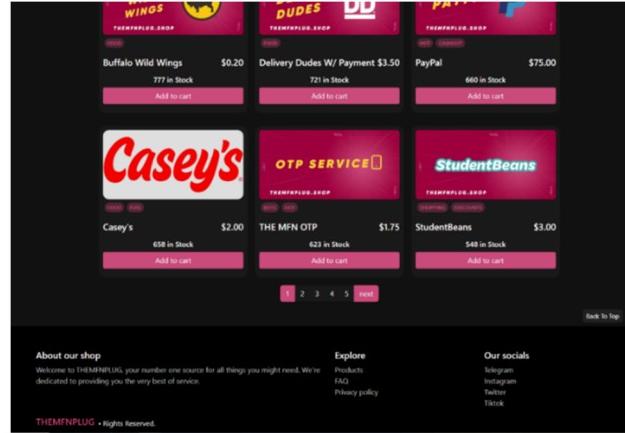


Photo-2

45. Photo-2 contains a list of “our socials” in the bottom right corner. The link for “Instagram” directs a user to the Instagram page for “them7nplug” (the “MFNPlug Instagram”). I recognize the name of the MFNPlug Instagram to be identical to TheMFNPlug, except that the number “7” has replaced the letter “F.” I have reviewed the MFNPlug Instagram and viewed the following photographs in a video posted to that Instagram:

Photo-3¹⁶

Photo-4

¹⁶ The name of the Betting Website has been redacted in certain of the photos in this complaint.



Photo-5



Photo-6

46. I know from my training and experience and involvement in the investigation that:

a. Photo-3 says, “[the Betting Website] HITTING.” I understand this to mean that users have been successful in stealing funds from hacked Betting Website accounts.

b. Photo-4 says, “[the Betting Website] Restock only @ themfnplug.io[.] 40K value in accounts all valid and can be cashed out with method in description! Don’t settle for 25% tax on Cashapp – settle for 25% off crypto through 😊[.] # [the Betting Website] #cashout #scam #accountshop #account #mk5plug #a7plug #kdmplug #fyp #viral #themfnplug.” Photo-4 further shows a large quantity of United States currency. I understand this message to mean that TheMFNPlug Shop was selling stolen Betting Website account with a total value of approximately \$40,000.

c. Photo-5 shows an individual withdrawing \$1,030 in stolen funds from a hacked Betting Website account.

d. Photo-6 shows an individual withdrawing \$1,004.44 in stolen funds from a hacked Betting Website account.

e. I generally understand these photos to be advertisements by TheMFNPlug for individuals to purchase access to hacked Betting Website accounts on the MFNPlug Shop

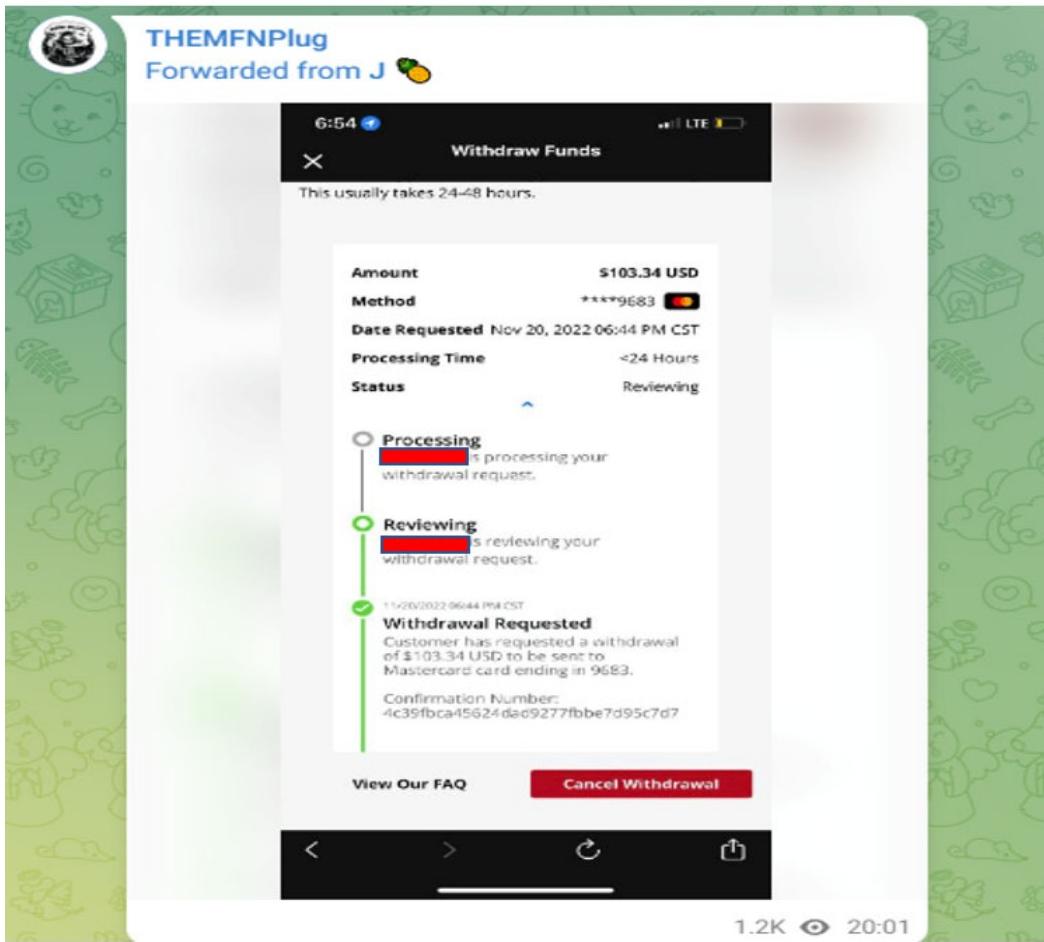
47. As described above, Photo-2 contains a list of “our socials.” One of those links is for a public message thread labeled “THEMFNPlug” on Telegram, an encrypted messaging application. I have reviewed that message thread, which contains the following:

a. On or about November 19, 2022, approximately one day after the Betting Website Attack, the user “THEMFNPlug” posted a list of approximately 26 usernames, passwords, and account balances, followed by the name of the Betting Website. Based on my

training and experience and involvement in the investigation, I understand this to refer to hacked Betting Website accounts available for sale on the MFNPlug Shop.

b. On or about November 21, 2022, approximately three days after the Betting Website Attack, the user “THEMFNPlug” messaged, “[the Betting Website] price lowered, go buy and hit before they patch it 🐱”

c. In the days following the Betting Website Attack, the user “THEMFNPlug” messaged multiple photos showing users stealing money from hacked accounts. An example of such a photo is below:



d. On or about October 21, 2022, approximately three days after the Betting Website hack, the user “THEMFNPlug” messaged a photo of a statement issued by the Betting Website regarding the Betting Website Attack, followed by “Mfn jus gon stop touching sites everytime I do the ceo wanna come out and say some. Bullshit statement.”

III. Evidence that “TheMFNPlug” is KAMERIN STOKES

48. I have reviewed a subpoena return from Coinbase for a Coinbase account with the username “themfnplug.” The account lists the name “Kamerin Stokes,” and the social

security number and date of birth of KAMERIN STOKES, a/k/a “TheMFNPlug,” the defendant. The subpoena return further showed that the account had received cryptocurrencies with a total value of over \$1 million.

49. I have reviewed a subpoena return from Cloudflare¹⁷ for a Cloudflare account for the MFNPlug Shop. The subpoena return shows that the Cloudflare account was paid for with a credit card in the name of “Kamerin Stokes.”

50. I have reviewed a subpoena return from Instagram for the MFNPlug Instagram. The subpoena return lists the name of the user as “Kamerin Stokes.”

51. I have reviewed a message on “THEMFNPlug” Telegram chat on or about February 18, 2023, in which the user “themfnplug” posted a mugshot photo of an individual. I have reviewed a mugshot photo for the arrest of “Kamerin Stokes” by the Shelby County, Tennessee, Sheriff’s Office from on or about December 22, 2022 that matches the mugshot photo posted on the Telegram chat.

52. I have reviewed subpoena returns for bank accounts and CashApp accounts showing that a CashApp account with the name “themfnplug” made multiple payments to bank accounts in the name of “Kamerin Stokes.” The bank subpoena returns further show that approximately \$1.5 million was deposited into bank accounts belonging to KAMERIN STOKES, a/k/a “theMFNPlug,” the defendant, between 2018 and 2023, although not all those funds came from the CashApp account.

53. Based on my review of subpoena returns for bank accounts, email accounts, CashApp accounts, and Cloudflare accounts, I have learned that KAMERIN STOKES, a/k/a “theMFNPlug,” the defendant, used the same internet protocol addresses (“IP addresses”) to log into his own bank accounts and various accounts associated with the alias “theMFNPlug.” For example:

a. Between in or about December 2022 and February 2023, STOKES logged into a Navy Federal Credit Union account in his name using the IP address 73.5.104.237. In the same time frame, that same IP address was used to log into the email accounts themfnplug.business@gmail.com and itsmfnkam@gmail.com.

b. Between in or about November 2022 and December 2022, STOKES logged into a Navy Federal Credit Union account in his name using the IP address 76.138.97.198. In the same time frame, that same IP address was used to log into the email account itsmfnkam@gmail.com and the Cloudflare account for the MFNPlug Shop.

¹⁷ Cloudflare is a technology company that provides various services to websites, including protection from distributed denial of service attacks.

WHEREFORE, the deponent respectfully requests that warrants be issued for the arrest of NATHAN AUSTAD, a/k/a "Snoopy," and KAMERIN STOKES, a/k/a "TheMFNPlug," the defendants, and that they be arrested and imprisoned, or bailed, as the case may be.

/s by the Court with permission

MICHAEL GASSERT
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission
of this Complaint by reliable electronic
means, pursuant to Federal Rules of
Criminal Procedure 41(d)(3) and 4.1, this
12th day of January, 2024

RTann
THE HONORABLE ROBYN F. TARNOFSKY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK